REMARKS

By this Amendment, Applicants cancel claim 14 without prejudice or disclaimer of the subject matter thereof. Applicants also amend claims 4, 5, 7-12, and 17-23, and add new claims 24 and 25 to address other aspects of the present invention. Upon entry of this Amendment, claims 4, 5, 7-13, and 17-25 will be pending.

In the Final Office Action mailed June 17, 2004, the Examiner rejected claims 4, 5, 7, 9, 11-14, 18, and 20-23 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,199,069 to Barrett et al. (hereinafter "Barrett") in view of U.S. Patent Application Publication No. 2000/0046564 to Masuda et al. (hereinafter "Masuda") and further in view of U.S. Patent No. 6,249,866 to Brundrett et al. (hereinafter "Brundrett") and further in view of U.S. Patent No. 6,649,025 to Epstein et al. (hereinafter "Epstein"), and rejected claims 8, 10, 17, and 19 under 35 U.S.C. § 103(a) as unpatentable over Barrett in view of Masuda and further in view of Brundrett and further in view of Epstein and further in view of U.S. Patent No. 4,484,025 to Ostermann et al. (hereinafter "Ostermann"). Applicants respectfully traverse the Examiner's rejections.

Regarding Claim Rejections

Applicants respectfully traverse the Examiner's rejection of claims 4, 5, 7, 9, 11-14, 18, and 20-23 under 35 U.S.C. § 103(a) as unpatentable over Barrett in view of Masuda and further in view of Brundrett and further in view of Epstein. In order to establish a prima facie case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim elements. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Third, there must be a reasonable expectation of success. See M.P.E.P. § 2143.

Independent claims 22 and 23, as amended, recite combinations including, for example, "a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm." Barrett fails to teach or suggest at least "a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm," as required by amended claims 22 and 23.

Barrett discloses an automatic encryption selector of a radio by using encryption hybrids to process received data stream. "The binary signal is then sent to the encryption hybrid (124 or 122) which had been previously selected by the user (as by the conventional operation of a switch on the radio). Encryption hybrids 122 or 124 are encryption circuits, and in particular, they are circuits capable of storing algorithms which allow for the encryption and decryption of messages (signals) which are transmitted or received respectively by radio 100." Barrett, column 3, lines 54-61, emphasis added. However, Barrett does not teach or suggest at least "a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm," as recited in claims 22 and 23.[1]

Masuda fails to cure Barrett's deficiencies. Masuda teaches "a storage medium accessible by the user outside an external storage device" and a decrypting algorithm "stored in an area inaccessible by the user outside the external storage device." Masuda, abstract. Masuda merely describes a method where: "[a] medium 35 for storing an algorithm 34 encrypted together with the data 17 is provided in the driver unit 12. A loader 31 in the device driver 22 loads the encrypted algorithm 34 into the PC 11, transmits it to the server 33, and requests the server 33 to decrypt the algorithm 34. Then, the loader 31 receives the algorithm decrypted by the sever 33 . . . ." Masuda, para. [0046]. However, Masuda's mere teaching of an encrypted algorithm does not constitute "a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm," as required by claims 22 and 23.

Brundrett fails to cure both Barrett and Masuda's deficiencies. Brundrett teaches an encrypted file system, "when the system receives a request to write any plaintext file data to disk in an encrypted manner, the file system receives the file data, encrypts the file data into encrypted file data to the disk." Brundrett, column 2, lines 30-34. In Brundrett, "[t]he encryption key is a random number encrypted by the public key of at least one user and at least one recovery agent" and "[t]hese keys are stored with the

[1] The Examiner recognized this by stating "[Barrett] but fail to show: (a) a cryptographic algorithm decryption means of decrypting the encrypted cryptographic algorithm." (Office Action at 3.)

file, whereby the file can always be decrypted by the private key of either a user or a recovery agent." Brundrett, column 2, lines 40-45. However, this single encryption key, encrypted by different public keys, does not constitute "a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm," as required by claims 22 and 23.

Epstein, as well, fails to cure the deficiencies of Barrett, Masuda, and Brundrett. Epstein teaches a method to distribute public/private key pairs. "A list of public/private key pairs are stored at a server, wherein the private key is stored in an encrypted form, the encryption being based on a master key." Epstein, abstract, emphasis added. "When a public/private key pair is required to be distributed to a new user, an administrator having the master key M 201 accesses the server 150, via a client processor 111 that is convenient to both the administrator and the new user." Epstein, column 4, lines 12-15, emphasis added. Epstein's teaching of distribution of public/private key pairs, however, does not constitute "a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm," as required by claims 22 and 23.

Moreover, Barrett, Masuda, Brundrett, and Epstein, being dissimilar technical applications, fail to suggest the desirability of at least the combination of "a key information storage section," which retains the encrypted key used for decrypting the encrypted cryptographic algorithm in addition to an encrypted encryption/decryption key used for cryptographic communication.

Therefore, none of Barrett, Masuda, Brundrett, and Epstein, taken alone or in any reasonable combination, teaches or suggests all elements recited by claims 22 and 23. A prima facie case of obviousness cannot be established regarding claims 22 and 23. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 22 and 23. Since claims 4, 5, 7, 9, 11-13, 20, and 21 depend on claim 22, either directly or indirectly, and claim 18 depends on claim 23, Applicants also request withdrawal of the rejection of claims 4, 5, 7, 9, 11-13, 18, 20, and 21 for at least the same reasons stated above. Since claim 14 has been canceled, the rejection of claim 14 is therefore moot.

Applicants also respectfully traverse the Examiner's rejection of claims 8, 10, 17, and 19 under 35 U.S.C. § 103(a) as unpatentable over Barrett in view of Masuda and further in view of Brundrett and further in view of Epstein and further in view of Ostermann.

Claims 8, 10, 17, and 19 depend, either directly or indirectly, from claim 22 or claim 23. As explained above, Barrett, Masuda, Brundrett, and Epstein fail to teach or suggest at least "a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm," as required by claims 22 and 23. Ostermann fails to cure the deficiencies of Barrett, Masuda, Brundrett, and Epstein. Ostermann teaches "[a] system and method for transmitting enciphered data between first and second terminals over a data transmission channel." Ostermann, abstract. Ostermann merely mentions that "[t]cipher algorithm is transmitted form the cipher program storage 18 over a data transmission channel 20 to the program memory 22 . . . ." Ostermann, column 2, lines 38-40. However, Ostermann does not teach or suggest at least "a key information storage section for storing and outputting the encrypted encryption/decryption key used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm," as required by claims 22 and 23.

Therefore, none of Barrett, Masuda, Brundrett, Epstein, and Ostermann, taken alone or in any reasonable combination, teaches or suggests all elements recited by claims 22 and 23. A prima facie case of obviousness cannot be established regarding claims 22 and 23. Since claims 8 and 10 depend on claim 22; and claims 17 and 19 depend on claim 23, Applicants respectfully request withdrawal of the rejection of claims 8, 10, 17, and 19 for at least the same reasons stated above.

Regarding New Claims

Applicants add claims 24 and 25 to address other aspects of the present invention. Support for claims 24 and 25 may be found at, for example, pages 13 and 19 of the specification. For at least the reasons stated corresponding to claim 22, claims 24 and 25 are neither anticipated nor rendered obvious by the prior art of record.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 16, 2004

By: Robert EConverse, Jr
Robert E. Converse, Jr.
Reg. No. 27,432